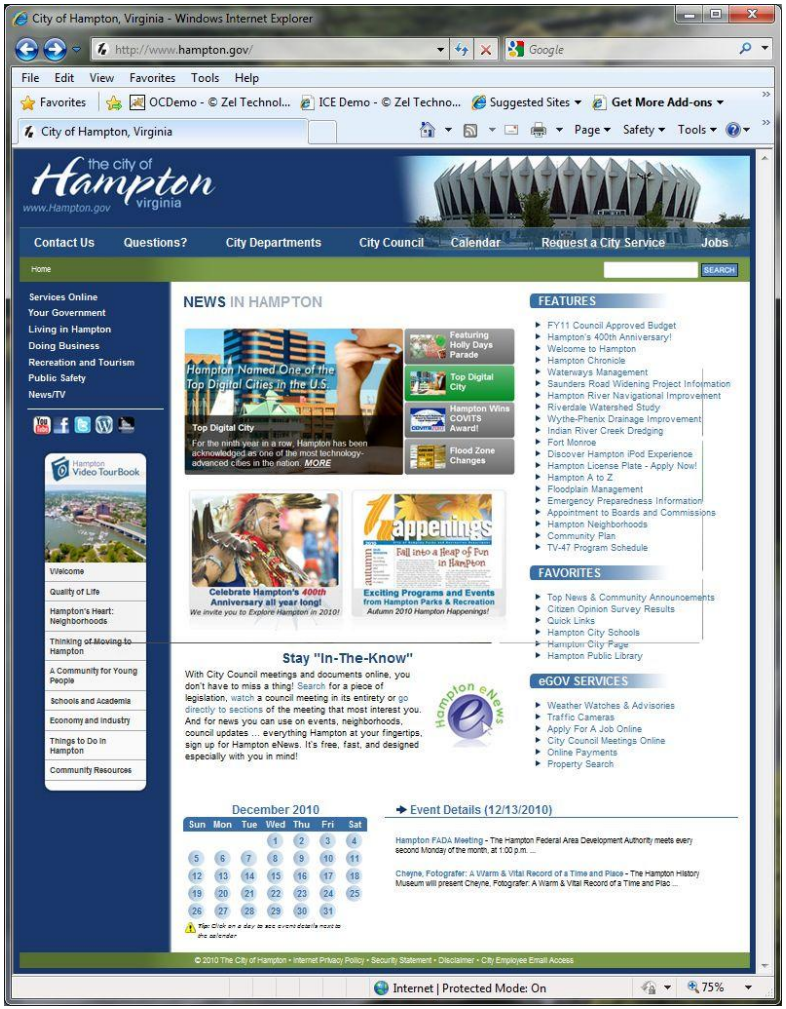
Virginia Operational Integrated Cyber Center of Excellence (VOICCE)

Ms. Leslie Fuentes
City of Hampton

Oct 16th, 2012

VOICCE Background

- **Cities are becoming accessible and "wired" as e-Gov is adopted. Services include:**
  - Government-to-Citizen
  - Government-to-Business
  - Government-to-Government
  - Government-to-Employee
- **These transactions enhance convenience & access but also increase vulnerabilities**
  - Few efforts to date have focused on these emerging trends
- **As a "Top Digital City" in the US, Hampton approached DHS with a proposal to mitigate these risks**



VOICCE Overview

- **The purpose of VOICCE is to enhance cyber security at the local level due to counter increased threat and criminal activities aimed at municipalities. Key factors that must addressed include:**
  - Appropriate policies and procedures must be developed to assist in the identification, development and evaluation of realistic processes to manage and enhance cyber security.
  - Affordable, effective technical measures need to be identified in parallel with real-world assessments that help balance risk and cost.
  - Primary thrusts oriented around day-to-day management, incident response (detect, characterize, respond, recover), and training/awareness.
- **The VOICCE lab provides the facility, equipment and models to:**
  - Identify and evaluate affordable, effective technologies and processes for municipalities, small businesses, and citizens alike.
  - Plan and manage evaluations and exercises with local government partners (technical and emergency management), industry, and academia.
  - Serve as clearinghouse for threat and defensive information for municipalities, small business, and citizens.

VOICCE Tasks

The VOICCE grant directed four tasks:

- Develop and stand-up a municipal cyber lab to support cyber vulnerability analyses, exercises, experiments, and models.
- Plan and execute two municipal Cyber Exercises or Evaluations.
- Develop and maintain a website for information sharing.
- Work with other stakeholders to enhance local information security through Workforce Development.

Lab Stand Up

- **Establish an initial municipal cyber lab with a high-level model of the IT infrastructure of a typical city government at a level of detail in specific domains required to support the development and execution of 2-3 cyber scenarios over the period of performance.**
- **Status**:
  - **Continuing to operate the cyber lab**
    - Municipal network modeling tools installed and operational. Initial model built, now updating and ingesting products from recent highly detailed municipal network scan.
    - Installed OpenFISMA and infrastructure and remediation tracking model built.
    - Developed a Low-Cost, Open Source Security Operations Center.
    - Developed and published over 30 security policy templates for use by cities at no cost.
  - **Lab capability**
    - Three large screen TVs, projector and collaboration system in place.
    - VTC capability, web-meeting, and collaboration systems in-place.
    - Equipment in-place to support meetings, demos, experiments and analyses.
  - **Lab uses expanding**
    - Used to brief and mitigate selected security vulnerabilities after web site analysis.
    - Supported a number of “real-world” cyber security incident analyses and responses.
    - Hosted a COOP exercise for the VPA.
    - IBM provided training for Langley AFB personnel on advanced network security tools.
    - Supported a number of events and meetings for the City of Hampton.

Cyber Exercises/Evaluations

Grant required two events: Three are completed, fourth in planning.

- **Cyber Exercise/Evaluation #1 – A vulnerability assessment of an external municipal website completed.**
  - Although over 160,000 tests executed, few serious technical issues identified.
  - Risk analysis provided, most technical vulnerabilities had very low operational risk. Initial vulnerabilities remediated immediately, others being worked off by priority.
- **Cyber Exercise/Evaluation #2 – Continuity of Operations Plan Exercise executed in VOICCE lab to support VPA in Dec 2011.**
  - Scenario included the detection of an explosive device in the Norfolk World Trade Center resulting in the evacuation of a workspace. With no previous notification, personnel directed to report to VOICCE lab where they successfully operated for 2 days.
  - Exercise support provided on a non-interference basis at to VPA and VOICCE at no cost.
- **Cyber Exercise/Evaluation #3 – Detailed internal vulnerability scan and assessment in June/July 2012.**
  - Deployed a high-end, externally funded vulnerability scanner inside a municipality's perimeter to provide a detailed analysis of all internal vulnerabilities. Potential vulnerabilities identified and being analyzed for prioritization and remediation.
- **Cyber Exercise/Evaluation #4 – Malware incident response in planning.**
  - Real-world incident highlighted need to analyze and document response "best practice." Current plan is to analyze lessons learned, develop and exercise an incident/disaster response approach, and document suggested best practices.

VOICCE Website

- **Develop and maintain VOICCE website(s) and other communication channels to enhance cyber awareness by providing security information, cyber threat data and/or training for citizens and/or government officials.**
  - Provide trending and other analysis for cyber security planning to local government officials.
- ***Status – Ongoing / On Schedule:***
  - Public Website Operational.
  - Website Enhancements Continue.
    - Extending/Expanding Content.
    - Automated Municipal Cyber Security RSS Feed.
    - VOICCE Specific News RSS Feed.
  - Website used to distribute additional VOICCE materials.
    - VOICCE has published three informational guides and pamphlets.
    - IT Security Policy Templates being developed and are available on site.

VOICCE.net

Workforce Development

- **Develop options to improve information security through workforce development, training and education both regionally and across the Nation. As an example, in Virginia develop partnerships with academic partners in Hampton Roads and throughout Virginia, focusing on DHS and NSA-certified programs and local community colleges with information security programs.**
  - Promote cyber security awareness, highlighting the interdependencies between cyber and physical critical infrastructures, and between and among different sectors of the Nation's infrastructure.
- **Status – Ongoing / On Schedule:**
  - With personal support from past and present TNCC Presidents, their Workforce Development organization has made significant strides identifying and obtaining grants from the Virginia Community College system.
    - Two conferences have been held.
    - Two highly discounted CISSP Boot Camp being held.
    - The potential of providing the first formal SCADA community college course training in Nation is in exploration, co-sponsored by TNCC and VOICCE.
  - TNCC's partnership and aggressive pursuit of this grant requirement has freed up significant funds for other VOICCE products and is a factor in enabling the no cost extension.

Summary

- **Without question, VOICCE has surpassed all grant tasks.**
  - While funded by DHS for a one year period of performance, in-kind contributions and no cost events have doubled that duration.
  - All key tasks on or ahead of schedule.
    - Lab proved effective for experiments, exercises, collaboration and as a development and evaluation site for VOICCE, Hampton, the VPA and others.
    - An open source Security Ops Center was developed and is being documented for distribution. Other open source tools are in evaluation.
  - The grant directed two exercise/evaluation events and three have already been completed.
  - TNCC partnership reduced VOICCE costs and allowed two conferences to be held enhancing security awareness and training.
- **Most significant issue is follow-on funding. We have a good story and everyone that hears it, lauds the concepts and progress to date but the "Way Ahead" is not yet clear.**
  - VOICCE accomplished its mission to serve as a "Proof of Concept" and demonstrated how valuable "time-shared" technical resources could significantly enhance information security at the local level.
  - Time sharing allows cost sharing to provide this expertise in a cost effective manner but a transition to cost sharing is required.

QUESTIONS???

Points of Contact:

- Bruce Sturk, VOICCE Executive Director, City of Hampton, 757-772-6102, bsturk@hampton.gov
- Scott Arnott, VOICCE Program Manager, Zel Technologies LLC. 757-722-5565, sarnott@zeltech.com
- http://www.voicce.net